



# CVE-2020-14797

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2020-14797
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert_us@oracle.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-10-21 15:15:00 UTC
<b>Updated</b>	2022-05-13 14:57:00 UTC
<b>Description</b>	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions the

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	7-mode Transition Tool	-	All	All	All
Application	Netapp	7-mode Transition Tool	-	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All
Application	Netapp	E-series Santricity Storage Manager	-	All	All	All
Application	Netapp	E-series Santricity Storage Manager	-	All	All	All
Application	Netapp	E-series Santricity Web Services Proxy	-	All	All	All
Application	Netapp	E-series Santricity Web Services Proxy	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All

Hardware	Netapp	Hci Storage Node	-	All	All	All
Hardware	Netapp	Hci Storage Node	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All
Application	Netapp	Santricity Unified Manager	-	All	All	All
Application	Netapp	Santricity Unified Manager	-	All	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Snapmanager	-	-	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Jdk	1.7.0	update271	All	All
Application	Oracle	Jdk	1.8.0	update261	All	All
Application	Oracle	Jdk	11.0.8	All	All	All
Application	Oracle	Jdk	15	All	All	All
Application	Oracle	Jdk	1.7.0	update271	All	All
Application	Oracle	Jdk	1.8.0	update261	All	All
Application	Oracle	Jdk	11.0.8	All	All	All
Application	Oracle	Jdk	15	All	All	All
Application	Oracle	Jre	1.8.0	update261	All	All
Application	Oracle	Jre	1.8.0	update_261	All	All
Application	Oracle	Jre	1.8.0	update_261	All	All

## References

Reference	Source	Link
Debian -- Security Information -- DSA-4779-1 openjdk-11	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Oracle Critical Patch Update Advisory - October 2020	MISC	<a href="http://www.oracle.com">www.oracle.com</a>
[SECURITY] [DLA 2412-1] openjdk-8 security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>

OpenJDK: Multiple vulnerabilities (GLSA 202101-19) — Gentoo security	GENIOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
[security-announce] openSUSE-SU-2020:1893-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
October 2020 Java Platform Standard Edition Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [330080](#) IBM AIX Java Multiple Vulnerabilities (java\_mar2021\_advisory)
- [375285](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-1310)
- [375367](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-1198)
- [375466](#) IBM CICS Transaction Gateway Multiple Vulnerabilities
- [375815](#) Azul Java Multiple Vulnerabilities Security Update October2020
- [375983](#) Amazon Corretto Critical Patch Update (OCT2020)
- [377238](#) Alibaba Cloud Linux Security Update for java-11-openjdk (ALINUX2-SA-2020:0172)
- [377467](#) Alibaba Cloud Linux Security Update for java-1.8.0-openjdk (ALINUX2-SA-2020:0174)
- [377821](#) F5 BIG-IP Multiple Vulnerabilities (K35253541)
- [501104](#) Alpine Linux Security Update for openjdk8
- [501206](#) Alpine Linux Security Update for openjdk11
- [501214](#) Alpine Linux Security Update for openjdk7
- [501650](#) Alpine Linux Security Update for openjdk7
- [670417](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-1982)
- [670859](#) EulerOS Security Update for java-1.8.0-openjdk (EulerOS-SA-2021-1982)
- [750542](#) OpenSUSE Security Update for java-1\_8\_0-openjdk (openSUSE-SU-2020:2083-1)
- [750556](#) OpenSUSE Security Update for java-1\_8\_0-openjdk (openSUSE-SU-2020:2048-1)
- [750579](#) OpenSUSE Security Update for java-11-openjdk (openSUSE-SU-2020:1994-1)
- [750585](#) OpenSUSE Security Update for java-11-openjdk (openSUSE-SU-2020:1984-1)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**